La Fédération internationale d’athlétisme victime d’un piratage informatique

La Fédération internationale d’athlétisme victime d’un piratage informatique

L'entreprise qui a étudié l'attaque estime « avec un haut degré de certitude » qu'un groupe de pirates fortement lié à la Russie est responsable.

La Fédération internationale d'athlétisme (IAAF) a été victime d'un piratage informatique, a annoncé l'instance lundi 3 avril dans un communiqué.

Des *« accès à distance non autorisés au réseau de l'IAAF »* ont été détectés le 21 février et ont visé, toujours selon l'IAAF, les exemptions accordées à certains athlètes les autorisant à utiliser, pour raisons médicales, des produits interdits.

Selon l'IAAF, l'attaque a été menée par le groupe Fancy Bear (aussi connu, notamment, sous le nom de APT28). Sollicitée par *Le Monde* pour savoir quels éléments techniques avaient permis de réaliser l'attribution, l'entreprise qui a étudié l'attaque pour le compte de l'IAAF n'a pas souhaité fournir de détail et ne publiera aucun élément technique.

« Context Information Security surveille les outils, les techniques et les procédures de Fancy Bear/APT28 depuis des années, via nos propres investigations et à travers la collaboration avec de nombreux chercheurs et organisations de cybersécurité. Les conclusions de notre investigation nous donnent un haut degré de certitude quant à l'attribution de cette attaque à Fancy Bear/APT28 », a précisé l'un des porte-parole de l'entreprise.

Des « AUT » déjà visées par des piratages

Les activités de Fancy Bear sont suivies depuis maintenant près d'une décennie par de nombreuses entreprises de sécurité informatique. Un large faisceau d'indices concordants laisse voir que ce groupe est lié à l'appareil d'Etat russe. Ce lien n'a cependant jamais été formellement prouvé.

La Fédération internationale d'athlétisme a suspendu depuis le 13 novembre 2015 la Russie de toutes les compétitions internationales – dont les Jeux olympiques de Rio et les Championnats du monde 2017 à Londres – après des révélations établissant un dopage d'Etat en Russie.

Le président de l'IAAF, le Britannique Sebastian Coe, a présenté *« les plus sincères excuses »* aux athlètes victimes du piratage et *« qui avaient confié à l'IAAF des informations qu'ils pensaient en sécurité et confidentielles »*.

Le système d'*« autorisations d'usage à des fins thérapeutiques (AUT) »* avait déjà été visé par des pirates ces derniers mois. A l'automne 2016, la base de données Adams, le système de gestion et de localisation de l'Agence mondiale antidopage (AMA), avait été piratée. Un groupe, se présentant sous le nom de Fancy Bear, avait ensuite publié par vagues successives les noms des sportifs bénéficiant d'AUT, parmi lesquels Rafael Nadal, Serena Williams, Simone Biles, Bradley Wiggins ou encore Christopher Froome…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *La Fédération internationale d’athlétisme victime d’un piratage informatique*

Alerte : un ransomware sur Android trompeur arrive à échapper aux antivirus

	Alerte : un ransomware sur Android trompeur arrive à échapper aux antivirus

---

Des chercheurs en sécurité ont trouvé un ransomware pour Android, capable d'éviter la détection par les antivirus. Il n'est dans l'absolu pas considéré comme très dangereux mais, comme certains malwares actuels, pourrait représenter une tendance.
L'histoire des malwares n'est pas nouvelle. Si l'on en croit un rapport publié en février par Eset (éditeur notamment de NOD32), le nombre d'attaques par ce vecteur a augmenté de 50 % en 2016 sur la plateforme de Google. Une conjonction de facteurs en est responsable, mais l'utilisation des boutiques tierces et les méthodes visant à tromper l'utilisateur sont clairement les plus présentes.

Des évolutions que l'on retrouve dans un nouveau ransomware découvert par la société ZScaler.
Rappelons – s'il est encore besoin de le faire – qu'il s'agit d'un logiciel malveillant dont l'objectif est de chiffrer les données de l'utilisateur puis de lui réclamer une rançon. Il peut payer et avoir une chance de les retrouver, ou refuser et faire avec les conséquences. Les sauvegardes régulières et une bonne hygiène informatique sont les deux seules armes vraiment efficaces contre ce type de menace.

Un compte à rebours de quatre heures

…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Android : un ransomware trompeur arrive à échapper aux antivirus*

Alerte : Une publicité sur Skype propage un rançongiciel

Alerte : Une publicité sur Skype propage un rançongiciel

Selon plusieurs utilisateurs, un logiciel malfaisant serait répandu via une publicité sur Skype par Roman De Schrijver

© Reddit

La publicité en question se présente comme une fausse page web d'Adobe. Ensuite, une fenêtre émergente surgit demandant de mettre à jour Adobe Flash Player. Si les utilisateurs se laissent tenter, c'est en réalité un maliciel qui s'installe sur leur ordinateur. Selon toute vraisemblance, ce maliciel est plutôt un rançongiciel (ransomware), à savoir un programme qui verrouille votre ordinateur et crypte vos données, de telle sorte que vous ne puissiez vous-même plus y accéder.

On ne sait pas encore à ce jour combien de victimes la fausse publicité a faites. Ce n'est du reste pas la première fois que les utilisateurs de Skype sont confrontés à ce genre d'annonce factice. Quoi qu'il en soit, il vous est toujours conseillé de rester vigilant vis-à-vis de ce que vous téléchargez et des liens sur lesquels vous cliquez.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Une publicité sur Skype propage un rançongiciel – ICT actualité – Data News.be*

Les bonnes pratiques pour lutter contre la cybercriminalité

Les bonnes pratiques pour lutter contre la cybercriminalité

Les entreprises modernes sont très vite confrontées aux dangers que représente un modèle commercial actif en permanence. Les clients ont de plus en plus recours à des outils en ligne pour accéder à des comptes, à des services ou à de l'expertise.

Quant aux employés, ils souhaitent pouvoir se connecter à distance et à tout moment aux réseaux de leur entreprise. D'où l'aspiration à un accès quotidien plus simple et plus pratique. Mais cette souplesse a aussi son revers. Les hackers, qui l'ont également bien compris, créent par conséquent des virus et des logiciels malveillants, dans l'unique intention de nuire. À la lumière des récentes révélations de l'organisme britannique Office for National Statistics selon lequel plus de 5,8 millions d'incidents de cybercriminalité ont eu lieu l'an dernier, il est crucial que les entreprises protègent les données de leur personnel et de leurs clients contre la cybercriminalité.
Dans ce contexte, quelles sont les principales activités de cybercriminalité dont les entreprises ont à se prémunir, et que faire pour les combattre ?

La manipulation sociale (Social engineering)
A l'ère du numérique, les pratiques de manipulation sociale sont devenues un problème préoccupant. Du fait que l'internet offre aux fraudeurs un voile d'anonymat, il est important que les sociétés qui détiennent des données clients sensibles soient au courant des pratiques les plus répandues parmi les hackers qui utilisent la manipulation sociale.
Le phishing aussi appelé hameçonnage, est peut-être la forme la plus connue de piratage de fraude par abus de confiance. Il recouvre les tentatives de fraudeurs qui généralement déploient de multiples moyens pour acquérir des données sensibles telles que les noms d'utilisateur, les mots de passe et les détails de paiement en se faisant passer pour une personne connue ou des organismes de confiance par courrier électronique ou une autre forme de communication numérique. Récemment, les cas de hameçonnage beaucoup plus ciblé, où les hackers se présentent comme des personnes de confiance, sont à la hausse. En cas de succès de l'attaque, les données des clients ou les documents sensibles d'une entreprise et donc sa réputation – sont en danger.
En effet, la recherche par Get Safe Online indique que la fraude liée au phishing a contribué aux organisations britanniques qui ont perdu plus de 1 milliard de livres sterling au cours de la dernière année en raison de la cybercriminalité.
Selon l'enquête, réalisée avec Opinion Way et dévoilée en exclusivité par Europe 1, 81% des sociétés française ont été ciblées par des pirates informatiques en 2015.
Le vishing et le smishing sont les variantes du phishing passant respectivement par les communications téléphoniques et SMS. Dans un cas comme dans l'autre, le principe est de récupérer les données sensibles de vos clients ou de votre entreprise. Compte tenu de l'impact dévastateur que peut avoir l'utilisation de la manipulation sociale par les cybercriminels sur les entreprises modernes, les dirigeants d'entreprise et les responsables informatiques doivent être très attentifs à ce type d'activités.

Menaces internes
A l'instar de la manipulation sociale qui peut porter préjudice aux entreprises de l'extérieur, il est légitime de se méfier également des menaces internes. Votre personnel peut disposer de privilèges d'accès aux données sensibles et en faire usage pour nuire à votre entreprise. Les employés mis à l'écart, les prestataires présents ou le personnel de maintenance sur site pourraient également représenter un danger pour votre société.
Les problèmes posés par les activités malveillantes des initiés ne sont pas toujours visibles immédiatement mais ils ne sauraient pour autant être ignorés. Prenons le cas d'un employé qui vient d'être licencié ou de perdre son poste dans une entreprise pour une autre raison. Il est possible que cette décision provoque chez lui de la colère et l'amène à vouloir exprimer son ressentiment envers son ancienne société. S'il possède toujours les droits d'accès au stockage partagé ou à des documents, il a la possibilité de modifier, supprimer ou falsifier les données ultrasensibles. De même, un prestataire exerçant sur le site et auquel un mot de passe temporaire a été attribué sans restrictions pour une courte durée peut représenter un danger. Qu'il s'agisse de corruption ou de communication de données financières, d'informations clients ou bien de droits d'authentification, les agissements de tels escrocs peuvent faire des ravages sur les entreprises de toutes tailles.
Cependant, comme c'est le cas avec les dangers de la manipulation sociale, le fait de connaître et de mesurer la menace potentielle des initiés malveillants peut permettre de faire un grand pas en avant dans la prévention des activités de cybercriminalité visant les entreprises. Les responsables informatiques et les dirigeants d'entreprises doivent rester vigilants en accordant aux utilisateurs des droits d'accès limités à leurs besoins et se méfier des récentes évolutions des techniques frauduleuses pour protéger leur entreprise contre les intentions malveillantes des cybercriminels.

Comment riposter
La lutte contre la cybercriminalité devrait dominer les débats et les plans stratégiques des dirigeants d'entreprise dans les années à venir. Pour optimiser leurs chances de l'emporter, les entreprises peuvent prendre plusieurs mesures.
1. Abandonnez la technique des mots de passe, trop simple, au profit d'un système d'authentification forte en entreprise : Les hackers qui dérobent le nom d'utilisateur et le mot de passe d'un employé peuvent la plupart du temps parcourir le réseau sans être repérés et charger des programmes malveillants ou bien voler ou enregistrer des données. Pour protéger les systèmes et les données, les entreprises ont besoin d'un système d'authentification forte qui ne repose pas exclusivement sur une information connue de l'utilisateur (mot de passe). Au moins un autre facteur d'authentification doit être utilisé, par exemple un élément que possède l'utilisateur (ex. un jeton d'ouverture de session informatique) et/ou qui le caractérise (ex. une solution d'identification biométrique ou comportementale). Il est également envisageable d'abandonner totalement les mots de passe et d'associer cartes, jetons ou biométrie.
2. Profitez de la commodité accrue d'un modèle d'authentification forte mobile : Les utilisateurs sont de plus en plus désireux d'une solution d'authentification plus rapide, plus transparente et plus pratique que celle offerte par les mots de passe à usage unique (OTP), les cartes d'affichage et autres dispositifs physiques. Désormais, les jetons mobiles peuvent figurer sur une même carte utilisée pour d'autres applications, ou être combinés sur un téléphone avec des dispositifs d'identification unique pour accéder à des applications cloud. Il suffit pour l'utilisateur de présenter sa carte ou son téléphone à une tablette, à un ordinateur portable ou à un autre périphérique pour s'authentifier sur un réseau, après quoi l'OTP devient inutilisable. Plus aucun jeton à mettre en place et à gérer. L'utilisateur final n'a qu'un seul dispositif à porter et n'a plus besoin de garder en mémoire ou de taper un mot de passe complexe.
3. Utilisez une stratégie de sécurité informatique par niveaux qui garantit des niveaux d'atténuation des risques appropriés : Pour une efficacité optimale, les entreprises ont intérêt à adopter une approche de la sécurité par niveaux, en commençant par authentifier l'utilisateur (employé, associé, client), puis en authentifiant le dispositif, en protégeant le navigateur et l'application, et enfin en authentifiant la transaction en recourant à l'intelligence basée sur les fichiers signatures si nécessaire. La mise en œuvre de ces niveaux nécessite une plateforme d'authentification polyvalente et intégrée dotée de moyens de détection des menaces en temps réel. Cette plateforme, associée à une solution antivirus, apporte le plus haut degré de sécurité possible face aux menaces actuelles.

_____

Chip Epps est Vice President, Product Marketing, IAM Solutions de HID Global
…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Les bonnes pratiques pour lutter contre la cybercriminalité Chip Epps, HID Global*

Rencontres cybersécurité à Toulouse le 10 mai 2017

Rencontres cybersécurité à Toulouse le 10 mai 2017

Le mercredi 10 mai, ToulÉco organise en partenariat avec la Région Occitanie / Pyrénées-Méditerranée et l'Anssi, l'Agence nationale de la sécurité des systèmes d'information, la troisième édition des rencontres cybersécurité d'Occitanie.

Objectif : sensibiliser et informer les entreprises et les collectivités sur les dangers liés à la cybersécurité et faciliter les échanges entre les différents acteurs. Parrainé par le Général Marc Watin-Augouard, fondateur et codirecteur du Forum international de la cybersécurité de Lille, cette journée aura pour thème « les nouveaux défis de la cybersécurité ».
Des ateliers grand public pour les dirigeants et des ateliers techniques pour les experts se dérouleront tout au long de la journée. A noter également un village d'exposants, et un concours à démo innovante qui fait partie des nouveautés de cette nouvelle édition.
Le mercredi 10 mai de 8h30 à 18h, au conseil régional d'Occitanie, 22 boulevard du Maréchal Juin à Toulouse. Entrée gratuite sur inscription.
Inscription gratuite
Plus d'infos, sur le site des Rencontres

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

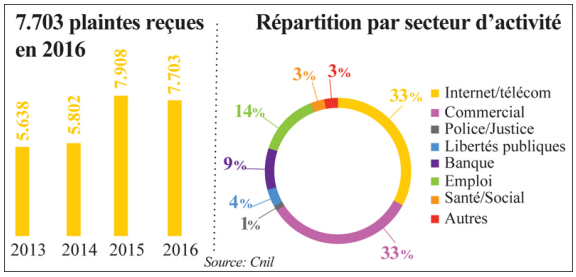
Source : *Les Rencontres cybersécurité d'Occitanie – ToulÉco*

Protection des données personnelles : Ce qui change en 2018 avec le règlement RGPD

Protection des données personnelles : Ce qui change en 2018 avec le règlement RGPD

Le nouveau règlement européen sur la protection des données personnelles entrera en vigueur le 25 mai 2018. «Ce texte rénove la régulation européenne des données et offre à l'Europe la possibilité de récupérer sa souveraineté numérique…», indique Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés (Cnil).

Le règlement renforce les droits des personnes à l'ère numérique
Les entreprises doivent se préparer au nouveau cadre juridique
Entrée en vigueur en mai 2018



En 2016, la Cnil a enregistré 7.703 plaintes (un peu moins que le record de 2015, 7.900 cas). Elles ont concerné principalement les secteurs Internet/télécom et le commerce
«La complexité du règlement avec ses 99 articles et ses 200 considérants ne doit pas masquer pour autant l'essence du texte qui consiste à renforcer la place centrale de l'individu dans l'univers des données», dit-elle. Pour le cas de la France, un projet de loi devra être déposé au Parlement au plus tard en juin 2017 pour garantir une meilleure application du règlement.
■ **Nouveau cadre juridique:** Le règlement européen constitue une évolution du cadre juridique de la protection des données et permet de construire une régulation commune sur l'ensemble du territoire de l'Union. Globalement, le texte renforce l'obligation des organismes publics et privés de protéger les données personnelles de leurs utilisateurs et clients. En pratique, le droit européen s'appliquera chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par Internet. La territorialité du droit européen se construit donc désormais autour de la personne. Cela se traduit par l'apparition de nouveaux droits (portabilité des données, limitation du traitement, réparation d'un dommage matériel ou moral…). Les obligations en matière d'information sont également renforcées notamment en cas de faille de sécurité.
■ **L'expression du consentement renforcée:** Les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer. La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambiguë. Le but de cette évolution est d'améliorer l'information qui doit être claire et accessible aux personnes concernées par les traitements de données.
■ **Portabilité des données:** Ce nouveau droit permet à une personne de récupérer les données qu'elle a fournies sous une forme facilement réutilisable, et, le cas échéant, de les transférer ensuite à un tiers. Il s'agit de redonner aux personnes la maîtrise de leurs données et de compenser en partie l'asymétrie entre le responsable de traitement et la personne concernée.
■ **Protection des enfants:** L'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Les Etats membres peuvent abaisser cet âge par la loi, sans toutefois qu'il puisse être inférieur à 13 ans. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.
■ **Biométrie:** Les données biométriques doivent faire l'objet d'une vigilance particulière. Le règlement européen a consacré le caractère particulier de ces données en les qualifiant de données «sensibles», au même titre que les données concernant la santé, les opinions politiques ou les convictions religieuses, dont le traitement est par principe interdit sauf dans certains cas limitativement énumérés.
■ **Open data:** Si elle ne concerne pas initialement la protection des données à caractère personnel, le nouveau contexte numérique implique de mieux la prendre en compte. Et ce notamment au niveau de la mise à disposition des données comme de leur réutilisation, la protection de la vie privée. Le nouveau cadre juridique permet cette conciliation.
Les sanctions s'alourdissent
Les autorités de protection pourront imposer des amendes administratives (jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial d'une entreprise). Ces sanctions pécuniaires pourront être prises en complément ou à la place de nombreuses mesures correctrices (ordonner de communiquer à la personne concernée une violation de données, la rectification ou encore la suspension de flux de données vers un pays tiers). Effacer des données ou limiter le traitement ou encore retirer une certification sont sur la liste des dispositions… Ces mesures et sanctions ne seront plus limitées au responsable de traitement mais pourront également être prises à l'égard d'un sous-traitant. Dans l'hypothèse de traitements transfrontaliers, la Cnil travaillera avec d'autres autorités de protection afin qu'une seule décision de sanction soit adoptée par l'autorité chef de file.
[Article original de Fatim-Zahra TOHRY]

Réagissez à cet article

Source : *Protection des données personnelles: Ce qui change | L'Economiste*

Comment voler des données au moyens de scanners de bureau ?

Comment voler des données au moyens de scanners de bureau ?

Des chercheurs israéliens ont trouvé un moyen de pirater les scanners de bureau. Ils deviennent des relais pour commander des malwares et extraire des données.

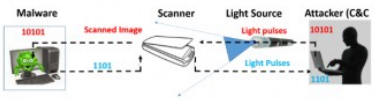
Jacques Cheminat

Décidément les universitaires israéliens sont passionnés par le piratage à distance avec des techniques dites 'Air Gap' (c'est-à-dire sans connexion à Internet). Récemment, une équipe avait démontré la capacité d'extraire des données depuis le clignotement des LED des disques durs de PC.

Quelques prérequis

Toujours dans les bureaux des entreprises, une autre équipe de chercheurs a jeté son dévolu sur les scanners. Ils ont piraté à distance un scanner pour qu'il puisse transmettre des commandes à un malware installé sur un PC en mode 'Air Gap'. Bien sûr la technique est valable dans l'autre sens, c'est-à-dire que le scanner peut être utilisé pour exfiltrer des données. Ils l'expliquent dans un document intitulé avec malice : « Oops… Je pense avoir scanné un malware »

La technique de piratage repose toujours sur la lumière. Dans le cas du scanner, un faisceau de lumière est considéré comme le binaire 1 et une absence de lumière comme le binaire 0. Pour réaliser leur expérience, les scientifiques attirent l'attention sur 2 éléments : le capot du scanner doit être ouvert pour qu'un laser puisse atteindre les capteurs des assaillants et un malware doit être installé sur un PC relié au scanner. Ce malware est programmé pour activer un scan à une date et heure précises. On est donc clairement dans une attaque ou un espionnage prémédité et ciblé.



Un laser ou via une ampoule connectée

Pour mener l'attaque, les chercheurs ont utilisé différents moyens. Ils ont ainsi mis un laser sur un drone et ont réussi à transmettre des données à une distance de 15 mètres. Avec un support fixe, cette distance est portée à 900 mètres. Ils ont testé également le piratage d'une ampoule connectée pour piloter le scanner et donner ainsi des instructions au PC compromis. Ce type d'attaques est imperceptible, constatent les chercheurs, car la variation de la lumière n'excède pas 5%.

Durant leurs tests, les chercheurs ont par exemple envoyé des commandes de suppression d'un PDF (d x.pdf) ou de chiffrement d'un dossier (en q). Les commandes ont pris entre 50 et 100 millisecondes pour être envoyées. La fuite de données est aussi possible à travers la lumière émise par le scanner, mais les chercheurs assurent que l'extraction est relativement difficile. Mais pas impossible.

[lire l'article original]

Réagissez à cet article

Source : *Quand les scanners se font complices des vols de données*

Piratage de McDonald’s Canada : les données personnelles de près de 100 000 demandeurs d’emploi volées

Piratage de McDonald’s Canada : les données personnelles de près de 100 000 demandeurs d’emploi volées

---

Après le compte Twitter il y a deux semaines, place au site Internet. Le site d'embauche de McDonald's Canada a été piraté et les données personnelles de près de 100 000 demandeurs d'emploi ont été dérobées, a annoncé la chaîne de restauration rapide.

Dans un communiqué, McDonald's rapporte que les données volées touchent les personnes ayant fait une demande d'emploi depuis mars 2014. Une cyber-attaque a eu lieu sur le portail de candidature, ce dernier recense les noms, adresses postales, adresses email, numéros de téléphone, historiques d'emploi, ainsi que d'autres renseignements liés à une candidature.

Pour tenter de rassurer, McDonald's note que les informations sensibles, comme le numéro d'assurance sociale, les renseignements bancaires et les renseignements sur la santé n'ont pas été volés. C'est assez normal après tout parce que McDonald's ne les demande pas lors des demandes d'emploi. Mais comme dit précédemment, la chaîne de restauration rapide tente de rassurer ses clients et les demandeurs d'emploi suite à l'attaque.

Dans l'immédiat, McDonald's Canada a décidé de verrouiller son portail de candidature, le temps de mener une enquête. Par ailleurs, la chaîne de restaurant ajoute que « rien n'indique que les renseignements saisis ont servi à un usage inadapté ». Elle invite les personnes voulant travailler à postuler directement dans ses restaurants plutôt que sur Internet pour l'instant…

Réagissez à cet article

Source : *Piratage de McDonald's Canada : les données personnelles de près de 100 000 demandeurs d'emploi volées | KultureGeek*

Big data. Comment les entreprises recueillent et utilisent nos données ?

Big data. Comment les entreprises recueillent et utilisent nos données ?

En 2015, 11 % des entreprises françaises ont traité des big data, selon l'Insee. Les sources de données les plus utilisées sont la géolocalisation, les médias sociaux et les objets connectés ou capteurs. Les grosses entreprises sont les plus à l'aise pour traiter ces données nombreuses et complexes.
Par Julie DURAND

1 % des entreprises françaises ont traité des big data en 2015. Selon l'Insee, qui a réalisé cette enquête, la big data est constituée de **» données complexes, dont le volume important et l'actualisation constante rendent difficile l'exploitation par les outils classiques «** .

7 % des entreprises traitent des données de géolocalisation

Sans surprise, les grosses entreprises sont plus nombreuses à en utiliser que les petites (24 % contre 9 %). Les barrières à l'utilisation de la data sont plus difficiles à franchir pour elles : mauvaise compréhension du sujet et de son intérêt, manque de compétences, coût trop élevé et législation contraignante.

La donnée la plus recueillie et la plus utilisée est la géolocalisation (pour 62 % des entreprises qui utilisent des data, soit 7 % de l'ensemble des entreprises françaises). Cette donnée intéresse surtout les entreprises de transports (92 %) et la construction (89 %).
Deuxième source : les médias sociaux (pour 32 % des entreprises qui utilisent des data, soit 4 % de l'ensemble). Ces données intéressent surtout l'hébergement-restauration (76 %) et l'information-communication (64 %).
Enfin, les objets connectés et capteurs sont la troisième source de data (29 % des entreprises qui en utilisent, soit 3 % de l'ensemble), utilisés principalement par l'industrie (46 %).

Traitement en interne ou externalisée des données ?

74 % des entreprises qui traitent des données le font en interne et 42 % par des prestataires extérieurs, 16 % utilisent donc ces deux méthodes. Le choix entre traitement interne ou externe dépend du secteur et de la taille de l'entreprise. 90 % des entreprises de l'infomation-communication et 84 % des activités scientifiques et techniques le font en interne, **» car les employés sont probablement mieux formés pour cela que dans d'autres secteurs »**. Tous secteurs confondus, 83 % des entreprises de plus de 250 personnes traitent les data en interne, contre 73 % pour les moins de 250 salariés.
Selon l'Insee, les entreprises utilisent toutes ces données pour optimiser leurs processus internes, améliorer leurs produits ou services et/ou rendre plus efficace leur marketing ou leur gestion des ventes.

Réagissez à cet article

Source : *Big data. Comment les entreprises recueillent et utilisent nos données ?*

Le Sénat nigérian approuve le vote électronique pour les élections de 2019

La chambre supérieure du Nigéria, le Sénat a approuvé le vote électronique lors des futures élections organisées par la Commission électorale nationale indépendante (CENI), notamment les élections générales de 2019.

Le Sénat, qui a examiné le rapport de son comité sur la Commission électorale nationale indépendante (CENI) portant sur un projet de loi pour la modification de la Loi électorale no 6, 2010 et pour d'autres questions connexes, qui a été adopté lors de la plénière de jeudi, a également légalisé l'utilisation du lecteur de carte à puce électronique pour les prochaines élections.

La carte à puce électronique a été introduite lors des élections de 2015.

Selon le Sénat, la Commission a adopté le vote électronique à toutes les élections ou toute autre méthode de vote qui peut être déterminée par la Commission.

Le Sénat a ajouté que l'amendement exige le vote électronique sans ambiguïté, mais donne également au Conseil le pouvoir discrétionnaire d'utiliser d'autres méthodes s'il est impossible d'utiliser le vote électronique lors des élections.

[block id="24761" title="Pied de page HAUT"]

A Lire aussi :
Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?
La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ? Cliquez ici pour une demande de chiffrage d'Expertise

Vos expertises seront réalisées par **Denis JACOPINI** :

• Expert en Informatique **assermenté et indépendant** ;

• **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;

• ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;

• qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;

• et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Source : *Le Sénat nigérian approuve le vote électronique pour les élections de 2019 – Apanews.net*